UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/581,064	10/07/2002	Ahmet Mursit Eskicioglu	RCA88783	6883

24498 7590 07/12/2005

THOMSON LICENSING INC.
PATENT OPERATIONS
PO BOX 5312
PRINCETON, NJ 08543-5312

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 07/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/581,064	ESKICIOGLU ET AL.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 04/21/2005. Original application contained Claims 1-7. Therefore, presently pending claims are 1-7.

Response to Arguments

Applicant's arguments filed 04/21/05 have been fully considered but they are not persuasive because of following reasons.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., generating a scrambling key in (emphasis added) a smart card using a first seed value received by the smart card and a second seed value permanently stored in the smart card, and thus fails to render claim 1) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicant argued that Chaney says nothing about, and provides no teaching or suggestion, regarding secret sharing. This is not found persuasive. In the combination of Chaney and Shamir, Shamir teaches the secret sharing shown in the title (How to share a secret).

In addition applicant argued that Shamir, like Chaney fails to teach or suggest using both a permanently stored seed value and a received seed value in a predetermined function to implement secret sharing. This is not found persuasive. Shamir discloses an executive given a small magnetic card with one Di piece (Section 1 Introduction paragraph 4); therefore a permanently stored seed value. The section further discloses the signature-generating device

accepts any of the three of them in order to generate a temporary copy of the actual signature key. Therefore the key is generated form one permanently stored key and one received key. Shamir teaches further receiving the other parts of the key to generate the temporary key.

The applicant argues further that Shamir teaches against storing secret key shares in a signature-generating device. This is not persuasive. In Section 1 Introduction paragraph 4, Shamir discloses the executive saving the key on a small magnetic card, and therefore storing secret key shares in a signature. The reference teaches against storing the complete computed key that is computed from all the shares of the other members. The reference says that all the pieces are required to forge a signature therefore there is no need to protect the device. However, the expression "it need not be protected," does not rule out protecting the portion of the key and therefore create greater security.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, dividing the key into pieces and distributing the key provides a robust key management system (Shamir, Introduction). This would also decrease fraud because an unfaithful executive must have at least two accomplices in order to forge the company's signature scheme (Introduction paragraph 4).

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that Chaney and Shamir do teach or suggest the subject matter broadly recited in independent Claims 1 and 5. Dependent Claims 2-4 and 6-7 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action. Accordingly, rejections for claims 1-7 are respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chaney (6,035,037) in view Shamir.

In reference to claim 1, Chaney discloses a method for managing access to a signal representative of an event of a service provider, said method comprising:

Receiving said signal in a smart card, said signal being scrambled using a scrambling key (column 4 lines 18-21). Therefore a key that is permanently stored in the smart card.

Descrambling, in the smart card, said signal using said generated scrambling key to provide a descrambled signal (column 3 lines 8-21).

Although Chaney teaches the generation of a scrambling key (column 7 lines 11-13), a key that is permanently stored in the smart card, and the storage of an algorithm in the smart card, the reference does not explicitly express a key based on a first seed value received in said smart card and a second seed value; and receiving, in said smart card, data representative of a first seed value.

Shamir discloses a method of secret sharing in which the generation of a scrambling key wherein the key is divided into pieces. Each party possesses one piece. In obtain the key a threshold number of keys must be combined using the predetermined function q() (section 2 page 613).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to divide the key into pieces as in Shamir and express a key based on the received key, from the other parties, and combine it with the key stored in the smart card of Chaney. One of ordinary skill in the art would have been motivated to do this because dividing the key into pieces and distributing the key provides a robust key management system (Shamir, Introduction).

In reference to claim 5, Chaney discloses a system for managing access between a service provider and a device having a smart card coupled thereto, said device performing the steps of:

Receiving from the service provider a signal representative of an event, said signal being scrambled using a scrambling key (column 4 lines 18-21).

Receiving from the service provider data representative of descrambling data from the ECM packet (column 7 lines -15).

Receiving form the smart card the descrambled signal (column 6 lines 7-16). Chaney also discloses a system where the software, and therefore the algorithm, for descrambling data is stored within the smart card having a means for access control processing (column 7 lines 30-35).

Chaney does not expressly disclose the descrambling data received in the form of a first seed value which is selected from a Euclidean plane and whereby secret sharing is implemented.

Shamir discloses a system for generating a key for descrambling wherein a first seed is selected form a plane (Euclidean plane) and whereby secret sharing is implemented (section 2 page 613).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to divide the key into pieces as in Shamir and express a key based on the received key, from the other parties, and combine it with the key stored in the smart card of Chaney. One of ordinary skill in the art would have been motivated to do this because dividing the key into pieces and distributing the key provides a robust key management system (Shamir, Introduction).

In reference to claim 2, wherein said first and second seed values are points on a Euclidean plane.

Shamir discloses interpolation given points on a 2-dimensional plain (section 2 page 613) to generate the keys, therefore the first and second keys are points on a Euclidean plane.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to divide the key into pieces as in Shamir and express a key based on the received key, from the other parties, and combine it with the key stored in the smart card of Chaney. One

of ordinary skill in the art would have been motivated to do this because dividing the key into pieces and distributing the key provides a robust key management system (Shamir, Introduction).

In reference to claim 3, wherein the step of generating said scrambling key comprises calculating the Y-intercept of a line formed on said Euclidean plane by said first and second seed values.

Shamir discloses interpolation given points on a 2-dimensional plain (section 2 page 613) to generate the keys, therefore the first and second keys are points on a Euclidean plane.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to divide the key into pieces as in Shamir and express a key based on the received key, from the other parties, and combine it with the key stored in the smart card of Chaney. One of ordinary skill in the art would have been motivated to do this because dividing the key into pieces and distributing the key provides a robust key management system (Shamir, Introduction).

In reference to claim 4, Chaney discloses a system wherein said smart card has a card body having a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 and PCMIA card standards (Chaney column 7 lines 36-50 in combination with Fig. 2A).

In reference to claim 6, Chaney suggests a system wherein the device is a set-top box (Fig. 1).

In reference to claim 7, Chaney suggests a system wherein the device is a digital television or a digital videocassette recorder (Fig. 1 part 150 and 155 is sent to a display). A digital television is one type of display.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Thursday, July 07, 2005

KIM VU
SUPERVISORY PATENT EXAMINE
TECHNOLOGY CENTER 2100